PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-176436**
(43)Date of publication of application : **21.06.2002**

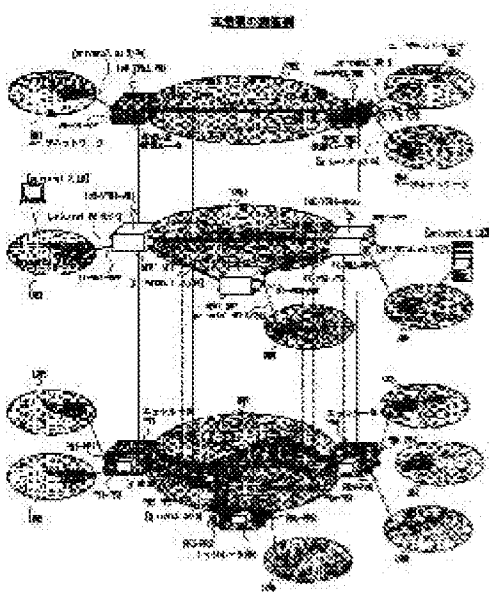
(51)Int.Cl. **H04L 12/56**
H04L 12/46
H04L 12/28

(21)Application number : **2000-371913**
(22)Date of filing : **06.12.2000**

(71)Applicant : **FUJITSU LTD**
(72)Inventor : **OGUCHI NAOKI**
SAITO TOMOTSUGU

(54) VIRTUAL CLOSED AREA NETWORK BUILDUP METHOD AND SYSTEM, AND REPEATER

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a virtual closed area network buildup method and system, and a repeater in a public data communication network that can eliminate the need for complicated VPN(Virtual Private Network) management and can be applicable to various tunnel technologies.
SOLUTION: When a sender repeater generates a control packet with a multicast address set thereto and multicasts the control packet and when a repeater whose address belongs to the multicast address receives the control packet, the repeater generates a virtual link to the sender repeater of the control packet, the repeater returns a reply packet via the virtual link to the sender repeater so as to generate virtual links all repeaters whose addresses belong to the multicast address thereby building up the virtual closed network.



LEGAL STATUS

[Date of request for examination] 13.11.2006

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－176436
（P2002－176436A）
(43)公開日　平成14年６月21日(2002.6.21)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/56		Ｈ０４Ｌ　11/20	１０２Ｄ	５Ｋ０３０
12/46		11/00	３１０Ｃ	５Ｋ０３３
12/28				

審査請求　未請求　請求項の数10　ＯＬ　（全 20 頁）

(21)出願番号　特願2000－371913(P2000－371913)

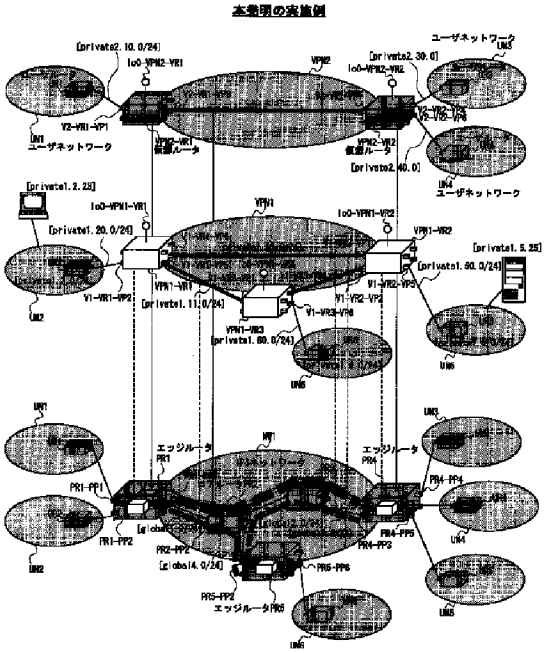
(22)出願日　平成12年12月６日(2000.12.6)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　小口　直樹
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　斎藤　友嗣
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(74)代理人　100090011
弁理士　茂泉　修司

最終頁に続く

(54)【発明の名称】　仮想閉域網構築方法及び装置並びに中継装置

(57)【要約】
【課題】、公衆データ通信網内の仮想閉域網構築方法及び装置並びに中継装置において、複雑なVPN管理が不要で且つ種々のトンネル技術に適用可能なようにする。
【解決手段】マルチキャストアドレスを設定した制御パケットが生成されてマルチキャスト され、該制御パケットが該マルチキャストアドレスに属する中継装置によって受信されると、該制御パケットの送信元の中継装置への仮想リンクが生成され、該仮想リンクを介して応答パケットが返送され、以て該マルチキャストアドレスに属する全ての中継装置間に仮想リンクが生成されることにより仮想閉域網を構築するように構成する。



1

【特許請求の範囲】
【請求項１】公衆データ通信網内で仮想閉域網を終端する各中継装置が仮想閉域網毎に予め定められたマルチキャストアドレスを設定した制御パケットを生成してマルチキャストし、
該マルチキャストアドレスに属する各中継装置が、該制御パケットを受信したとき、該制御パケットの送信元の中継装置への仮想リンクを生成し、該仮想リンクを介して応答パケットを返送し、
以て該マルチキャストアドレスに属する全ての中継装置間に仮想リンクが生成されて該仮想閉域網が構築されることを特徴とする仮想閉域網構築方法。
【請求項２】請求項1において、
該中継装置が受信した該制御パケットの認証を行うことを特徴とする仮想閉塞網構築方法。
【請求項３】請求項１において、
該仮想リンクがIPトンネル又はMPLSトンネルであることを特徴とした仮想閉域網構築方法。
【請求項４】公衆データ通信網内に仮想閉域網の構築を開始するときに、予め定められたマルチキャストアドレスを設定した該制御パケットを生成してマルチキャストする中継装置と、
該制御パケットを受信したとき、該制御パケットの送信元との間に仮想リンクを生成し、該仮想リンクを介して応答パケットを返送する中継装置とを備え、
各中継装置が作動して該マルチキャストアドレスに属する全ての中継装置間に仮想リンクが生成されることにより該仮想閉域網を構築することを特徴とした仮想閉域網構築装置。
【請求項５】請求項４において、
該仮想リンクを生成する中継装置が、受信した該制御パケットの認証を行うことを特徴とする仮想閉域網構築装置。
【請求項６】請求項４において、
該仮想リンクがIPトンネル又はMPLSトンネルであることを特徴とした仮想閉域網構築装置。
【請求項７】公衆データ通信網内で仮想閉域網を終端する中継装置において、
仮想閉域網毎に予め定められたマルチキャストアドレスを設定した該制御パケットを生成してマルチキャストする手段と、
該制御パケットを受信したとき、該制御パケットの送信元の該中継装置との間に仮想リンクを生成し、該仮想リンクを介して応答パケットを返送する手段と、
を備え、以て該マルチキャストアドレスに属する全ての中継装置間に仮想リンクを生成することにより該仮想閉域網を構築することを特徴とする中継装置。
【請求項８】請求項７において、
受信した該制御パケットの認証を行う手段をさらに備えたことを特徴とする中継装置。

2

【請求項９】請求項７において、
論理的に互いに独立した複数の仮想閉域網それぞれの経路表を生成する手段と、該経路表に基づいて各仮想閉域網のパケット中継を行う手段とをさらに備えたことを特徴とする中継装置。
【請求項10】請求項７において、
該仮想リンクがIPトンネル又はMPLSトンネルであることを特徴とした中継装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、仮想閉域網構築方法及び装置並びに中継装置に関し、特に公衆データ通信網内の仮想閉域網構築方法及び装置並びに中継装置に関する。
【０００２】
【従来の技術】複数地点に分散する拠点(ユーザ拠点)を有する企業等が各ユーザ拠点のローカルエリアネットワーク(LAN)を接続して社内ネットワーク等を構築するためのLAN間接続技術は従来よりさまざまな方法が採られて来た。
【０００３】例えば、各ユーザ拠点間を専用線で接続する専用線サービスが挙げられる。ところが、専用線サービスは非常に高価であり課金が距離に比例して行われるため、ユーザ企業は、利用回線距離をできるだけ節約するため、拠点を珠数つなぎにする形態のLAN間接続を行っていた。
【０００４】この場合、中間に位置するユーザ拠点が障害で通信不能になると、エンド・エンド間の通信も不通になるといった問題があった。その後、専用線に比べて料金が割安になるATMやFRといった仮想専用線サービスが登場し、距離に比例する課金ではなく、仮想コネクション数に応じた課金が行われるようになった。
【０００５】その結果、各支店(ブランチオフィス)のLANを本部(ヘッドクオータ)にスター型に接続するネットワーク構成が増え、中間拠点の障害により他の拠点が影響を受けることが減少した。さらに、インターネットの普及により、ユーザ企業はATMやFRといった仮想専用線サービスを利用しなくても、公衆データ通信網であるインターネットを利用して、分散するユーザ拠点を接続することが可能になった。このようなサービスは、インターネットVPNサービスと呼ばれ、物理的な接続拠点数により課金される。なお、VPNはVirtual Private Networkの略であり、仮想閉域網と称される。
【０００６】一般に、インターネットVPNサービスにおいて、各ユーザ拠点のLAN(以降、ユーザネットワークと称する。)ではプライベートアドレスを使用しているため、そのままではグローバルアドレスを持つインターネットにパケットを流すことはできない。
【０００７】そこで、複数のユーザネットワーク拠点間でグローバルインターネットを経由した通信を行うため

には、いわゆるトンネル技術が必要となる。すなわち、ユーザネットワークからグローバルインターネットへパケットを送信する際は、送信元のユーザネットワーク内のグローバル網接続ルータ(グローバルインターネットに直接接続されるルータ)において、送信するパケットをグローバルアドレスを持つIPパケットでカプセル化した後、グローバルインターネットを経由して宛先ユーザネットワークへ送信する。

【０００８】宛先ユーザネットワークのグローバル網接続ルータでは、このパケットを受信すると同時にカプセル化を解き(デカプセル化し)、宛先ユーザネットワーク内の宛先ホストコンピュータへルーティングする。この場合、各ユーザネットワークにおいて、トンネルを始終端可能な（カプセル化／デカプセル化可能な）装置であるグローバル網接続ルータを用意する必要があるが、処理が複雑になるとグローバル網接続ルータの性能が低下してしまうため、性能を上げるために高価な機器に買い替えたり、アップグレードを行わなければならないことになる。

【０００９】さらに、拠点が多数ある場合、経路制御、論理インタフェースの設定といったグロバールインターネットに接続するために必要な各種の設定がより複雑になって来る。この場合、ユーザ企業では、VPNを維持管理するための管理者を教育する必要があり、人員やコストがかかっていた。

【００１０】そこで、VPNの維持管理を公衆データ通信網のプロバイダ（Internet ServiceProvider、以下、ISPと略称する）或いはキャリアにアウトソースし、ユーザネットワークでは既存のルータをそのまま利用可能とする新たなVPNサービスが考えられている。以下、このようなVPNサービスをIP-VPN(Internet Protocol-Virtual Private Network)サービスと称する。

【００１１】IP-VPNサービスでは、トンネルの始終端機能を公衆データ通信網内の中継装置で提供する（以下、トンネルの始終端機能を有する公衆データ通信網内の中継装置をエッジルータと称することがある）。さらに、ユーザ拠点が複数あり、各拠点のユーザネットワークが異なるエッジルータに接続される場合は、或るユーザネットワークから送信されるパケットについて、どちらのトンネルへカプセル化されたパケットを送信すべきかを宛先ユーザネットワークに応じてエッジルータが判断するユーザネットワーク間の経路制御が必要となるが、この経路制御機能もエッジルータが提供する。

【００１２】すなわちエッジルータは、グロバールインターネットの経路情報とは別に、ユーザネットワークのプライベートアドレスの経路情報に基づきパケットを転送する。図21は、一般的なIP-VPNサービスを説明するために、ユーザネットワークがプライベートアドレスを用いて運用されている場合に、これらユーザネットワーク間を接続するトンネルにより構成される仮想的なネットワーク（以下、プライベートネットワークと称する）がグローバルアドレスを用いて運用されるインターネット（以下、グローバルインターネットと称する）にオーバレイされている様子を示したものである。

【００１３】同図において、グローバルアドレス空間を提供するISPネットワークNW1は、エッジルータPR1,PR4及びPR5、並びにコアルータ（ユーザネットワークを収容せず、トンネルの始終端機能を提供しない公衆データ通信網内のルータ）PR2及びPR3によってバックボーンが構成されている。

【００１４】ここで、或るユーザ企業が、IP-VPNサービスを利用してユーザネットワークUN1～UN6を接続したい場合を考える。このとき、各ユーザネットワークUN1～UN6内には既存のルータ(ユーザルータ)UR1～UR6が存在し、ユーザルータUR1及びUR2はエッジルータPR1に、ユーザルータUR3～UR5はエッジルータPR4に、ユーザルータUR6はエッジルータPR5にそれぞれ接続されている。

【００１５】各エッジルータPR1,PR4及びPR5内には、それぞれ仮想ルータVPN1-VR1～VPN1-VR3が存在している。従って、同図においてネットワークＮＷ1の上方に取り出して示す如く、各ユーザネットワークUN1～UN6はこれらの仮想ルータVPN1-VR1～VPN1-VR3を介してプライベートアドレス空間である仮想閉域網VPN1によって接続されている。

【００１６】このようなIP-VPNサービスとして従来から提案されている方式について以下に具体的に説明する。

(1)IETF RFC2547

まず、図22を用いて、IETF RFC2547として提案された方式について説明する。

【００１７】同図は、図21と同様の物理的な接続形態を有することを示している。但し、図22の場合は、図21と異なり、ユーザネットワークUR1,UR3,及びUR4を拠点とするユーザ企業(企業A)とユーザネットワークUR2,UR5,及びUR6を拠点とするユーザ企業(企業B)とが異なっている場合を想定している。

【００１８】従って、図22では、企業A用の仮想閉域網VPN2及び企業B用の仮想閉域網VPN1が別々に構築されている。また、同図においては、各エッジルータPR1,PR4及びPR5における物理インタフェースであるポートとして、例えばエッジルータPR1についてはポートPR1-PP1,PR1-PP2,及びPR1-PP6が示されている。

【００１９】各仮想ルータVPN1-VR1, VPN1-VR2, VPN2-VR1, 及びVPN2-VR2における仮想インタフェースであるポートについても、例えばVPN2-VR1についてはV2-VR1-VP1及びV2-VR1-VP6が示されている。以下に、このIETF RFC2547方式における処理内容を説明する。

【００２０】企業A及びBがそれぞれのユーザネットワーク間で通信を行う場合、ISPネットワークNW1を経由して各仮想閉域網VPN2及びVPN1においてパケットを転送する必要がある。RFC2547方式では、Multi Protocol Label

Switching(MPLS)と呼ばれる技術と、Border Gateway Protocolと呼ばれる経路制御プロトコルセスを用いてVPNを実現している。

【００２１】MPLSはIP経路上のルータにおいて、ネットワーク層で行われるIPパケット中継処理を、パケットに付加したラベルを用いてデータリンク層において行うラベル処理に置き換えることで、経路検索の処理を軽減し、高速なパケット中継を可能とする技術である。

【００２２】MPLSにおいては、ラベルはルータ間のリンクに対しリンクを共有するルータ間で取り決められた値であり、ルータは、ラベル付きパケットを受信すると、ラベルを見て中継先を決定し、出力リンクに対する新たなラベルをパケットに付加して再度送出する。

【００２３】ラベルによりパケットが転送されるパスをLabel Switching Path(LSP)と呼ぶ。これは、ラベルによりIPパケットがカプセル化され転送されるトンネルと考えることができる。以下ではLSPをMLSPトンネルと呼ぶ場合もある。また、RFC2547方式では、Border Gateway Protocol(以下、BGPと称する)と呼ばれる経路制御プロトコルを使用する。各エッジルータでは、このプロトコルを実現する経路制御プロセスが起動しており、各エッジルータ上の経路制御プロセスがフルメッシュで接続される。あるいは各エッジルータをスター状に接続し、フルメッシュ時と同様な経路制御パケットの交換を提供するルートリフレクタを介して接続される。

【００２４】MPLSによりこれら経路制御パケットを、フルメッシュに接続されたエッジルータ間で交換するためには、エッジルータ間にフルメッシュとなるようLSPを予め生成する必要がある。ここで作成されるLSPは、グローバルな宛先プレフィックスに対し経路上のルータ間リンクに対するラベルが各ルータに設定されることで実現されており、これをレベル1トンネルと呼ぶこととする。図22の構成では、PR1–PR4間、PR1–PR5間、PR4–PR5間にレベル1トンネルが生成される。

【００２５】プロバイダ管理者は、各エッジルータのポート(I/F)番号とユーザサイト識別子としてのRoute Distinguisher(以下、RDと称する)を対応付ける。この場合、RDは任意の番号で良く、プロバイダ網が管理するユーザネットワーク毎にユニークであれば良い。

【００２６】また、RD内で区別される各ユーザネットワークのどれとどれが同じVPNに属するかを設定した、各VPNに対するRDの集合の対応付けが別途あり、この対応付けにより、例えばエッジルータPR1のポートPR1–PP1及びPR1–PP2にはそれぞれVPN2及びVPN1が対応付けされることになる。エッジルータ内では各VPNをVPN番号で区別し、VPN番号はVPN毎に独立した経路表を管理したり、ユーザネットワークを収容するポートとVPNの対応をとるのに使用される。

【００２７】また、プロバイダ管理者は、ユーザネットワークと接続しているエッジルータのポート毎にポート番号と仮想ルータの仮想インタフェースを一対一に対応付ける。このような対応付けにより、例えばエッジルータPR1のポートPR1–PP1及びPR1–PP2にはそれぞれ仮想インタフェースV2–VR1–VP1及びV1–VR1–VP2が対応付けされることになる。

【００２８】なお、各エッジルータPR1,PR4,及びPR5は、VPN毎に独立した経路表を有している。これらは、VPN間で共通な経路制御プロセス(BGP)により、ローカル拠点あるいはリモート拠点から受信した全ての仮想閉域網(図22の場合はVPN1及びVPN2)内の経路情報に基づき仮想閉域網毎に独立して生成されるものである。

【００２９】この際、各エッジルータ上の経路制御プロセスは、送受信する経路情報のアドレスプレフィックスにRDを付与するため、仮想閉域網毎に経路情報を区別することができる。また、各エッジルータは、データパケットを受信したポート番号によりVPNに対応した経路表を検索し、受信したパケットをフォワードする機能を持つ。このフォワード機能は、パケットをエッジルータ間に生成したトンネルへ送信するための仮想インタフェースを有している。

【００３０】各エッジルータは、同一VPN内の宛先プレフィックス毎に異なるMPLSトンネル(レベル2トンネル)を持ち、宛先毎に異なるトンネルを識別することができる。エッジルータは、レベル1トンネルの中にネストして、同一エッジルータ区間を共有する各プレフィックス毎のトンネル(レベル2トンネル)を多重する。実際には、エッジルータは、レベル1トンネルとレベル2トンネルに対応したMPLSラベルをIPパケットに二重に付加して送信する。

【００３１】この様子は図22においてエッジルータPR1とPR4との間のレベル1トンネル内に3本のレベル2トンネルが生成されていることで分かる。すなわち、3本のレベル2トンネルとは、仮想ルータVPN2–VR1の仮想ポートV2–VR1–VP6と仮想ルータVPN2–VR2の仮想ポートV2–VR2–VP1との間にアドレスプレフィックス毎に生成された2本のトンネルと、仮想ルータVPN1–VR1の仮想ポートV1–VR1–VP6と仮想ルータVPN1–VR2の仮想ポートV1–VR2–VP1との間に生成された1本のトンネルである。

【００３２】各エッジルータ上のVPN毎の経路表には、宛先プレフィックスに対する次ホップエッジルータの代表アドレスと送信すべき仮想インタフェースが記述される。仮想インタフェースは、宛先エッジルータへ繋がるレベル2のトンネルの入り口である。

【００３３】図22において、エッジルータPR1内の仮想ルータVPN2–VR1の仮想インタフェースV2–VR1–VP6は、宛先エッジルータPR4へ繋がるレベル2のトンネルの入り口である。エッジルータは、プレフィックス毎に異なるラベルを付与すると共に、次ホップエッジルータの代表アドレスから決定されるレベル1トンネルのためのラベルも付加しグローバルインターネットへ繋がった物理ポー

ト(PP)に送信する。

【００３４】経路制御プロセスにおいては、各エッジルータ上の経路制御プロセスは、エッジルータ間に生成されたレベル1トンネルを通して、グローバルインターネット、及び各VPN毎の経路情報を交換し、VPN毎に独立した経路テーブルを生成する。フォワード処理については、ユーザ拠点からエッジルータの物理ポートにパケットが到着すると、エッジルータはパケットを受信した物理ポートに対応付けられたVPN番号から、VPNに対応する経路テーブルを参照し、次ホップエッジルータが接続される仮想インタフェースへパケットを送信する。

【００３５】仮想ルータが、仮想インタフェースへパケットを送信した場合、実際には、エッジルータは、プレフィックス毎のレベル2トンネルに対応したラベル（以下、レベル2ラベルと称する）を付加した後、宛先仮想ルータが搭載されているエッジルータへのレベル1トンネルに対応するラベル（以下、レベル1ラベルと称する）を付加し物理インタフェースに送信する。

【００３６】また、エッジルータがISPネットワークNW1からラベル付きパケットを受信した場合、ラベルにより次ホップルータ、出力物理ポートを決定する（ラベルによる中継処理を記したラベルテーブルが用いられる）。例えば、米国・シスコ・システムズ社のMPLS実装では1ホップ前のLSR(labelswitching router)でレベル1ラベルが外されるため、エッジルータは、レベル2ラベル付きのパケットを受信する。エッジルータはレベル2ラベルを見て、ラベルテーブルを検索しユーザ拠点の接続された物理ポートへパケットをフォワードする。この際レベル2ラベルは外されてフォワードされる。

【００３７】(2)IETF draft draft-muthukrishnan-core vpn-arch-00.txt

次に、図23を用いて、IETF draft draft-muthukrishnan-corevpn-arch-00.txtとして提案された方式について説明する。同図の構成は、図22とほぼ同様である。但し、仮想閉域網VPN2における、仮想ルータVPN2-VR1の仮想インタフェースV2-VR1-VP6と仮想ルータVPN2-VR2の仮想インタフェースV2-VR2-VP1との間のトンネルが図22では2本であるのに対し、図23では1本である点が異なっている。

【００３８】これは、この方式においては、宛先プレフィックス毎の管理を行っていないためである。また、この方式の場合は仮想ルータ間の経路制御プロトコルをBGPに限定していないため、必ずしもこれらのエッジルータ間でフルメッシュにトンネルを生成する必要はない。しかしながら、エッジルータに障害が起きたとき、エンド・エンド間通信を阻害することや、エッジルータを多く中継することで、中継されるパケットのルータホップ数が増してしまうことを考慮するとフルメッシュにトンネルを生成することが望ましい。

【００３９】この場合のトンネル技術としては、MPLS(multi protocol label switching)が使用され、プロバイダ管理者は、図22の場合と同様に、全エッジルータの組に対し、MPLSトンネル(レベル1トンネル)を生成する。また、図22の場合と異なり、各エッジルータではVPN毎に独立した仮想ルータ機能を動かし、同一VPNに属する仮想ルータは同一のVPN-IDが設定される。仮想ルータ機能は、ユーザネットワーク内の経路情報を受信し、これに基づいた経路表を生成するルーティング機能と、受信したポート番号によりVPN-IDに対応した経路表を検索し受信したパケットをフォワードするフォワード機能とを有している。このフォワード機能は、パケットをエッジルータ間に生成したトンネルへ送信するための仮想インタフェースを有している。

【００４０】また、各エッジルータ上の同一VPN-IDを持つ仮想ルータは、グローバルネットワーク上の仮想リンクを用いて接続されるが、他のVPN-IDを持つユーザ拠点からのトラフィックと区別するために、VPN毎に異なる仮想リンク(トンネル)を用いる(レベル2トンネル)。

【００４１】エッジルータは、レベル1トンネルの中にネストして、同一エッジルータ区間を共有する各VPNの仮想ルータ間リンク(レベル2トンネル)を多重する。実際には、エッジルータは、レベル1トンネルとレベル2トンネルに対応したMPLSラベルをIPパケットに二重に付加して送信する。

【００４２】各エッジルータ上の仮想ルータは、どのレベル2トンネルの先にどのエッジルータ上の仮想ルータが接続されているかを判断するために、レベル2トンネルのラベル値とトンネルの接続先である宛先仮想ルータの仮想I/Fのアドレス（仮想I/FにIPアドレスを割り振る場合）、あるいは宛先仮想ルータの代表アドレスが対応付けられる（ポイントツーポイントリンクの場合で仮想I/FにIPアドレスを割り振らない場合）。

【００４３】また、プロバイダ管理者は、ユーザ拠点と接続しているポート番号に対し、仮想ルータの仮想インタフェースを一対一に対応付ける。同一VPN-IDを持つ各仮想ルータは、エッジルータ間に生成されたレベル2トンネルを通して、相互の経路情報を交換し、VPN-ID毎に独立した経路テーブルを生成する。

【００４４】ユーザ拠点からエッジルータの物理ポートにパケットが到着すると、エッジルータはパケットを受信した物理ポートに対応付けられたVPN-IDから、VPN-IDに対応する経路テーブルを参照し、次ホップ仮想ルータが接続される仮想インタフェースへパケットを送信する。

【００４５】仮想ルータが、仮想インタフェースへパケットを送信した場合、実際には、エッジルータは、レベル2トンネルに対応したラベルを付加した後、宛先仮想ルータが搭載されているエッジルータへのレベル1トンネルに対応するラベルを付加し物理インタフェースに送信する。

【００４６】エッジルータがレベル1トンネルからラベル付きパケットを受信した場合は、エッジルータは、カプセル化されたパケットのレベル1ラベルを見て、自身宛か(ラベル削除)、フォワードか(ラベル付け替え)を判断し、自身宛の場合は、レベル2トンネルに対応するラベルを見て、エッジルータ内仮想ルータのどの仮想インタフェースで受信するかを決定する。この時、エッジルータはレベル2ラベルを外して仮想インタフェースに渡す。

【００４７】仮想インタフェースでパケットを受信した仮想ルータは、受信したIPパケットのIPヘッダの宛先アドレス（これはユーザネットワーク内の宛先アドレスである）を見て、仮想ルータの持つVPN用経路表を検索しパケットをユーザ拠点の接続された物理ポートに対応付けられた仮想インタフェースのいずれかへフォワードする。

【００４８】なお、上記(1)および(2)ではトンネル技術としてMPLSトンネルを用いている。この場合、MPLSトンネルが中継するパケットは図24に示す如くSHIMヘッダが二重に付加されたフォーマットになっている。しかしながら、MPLSトンネル以外のトンネル技術であるIPトンネルとしてL2TP(layer two tunneling protocol)トンネルやIPsec(IP security protocol)トンネルも一般的には利用されている。

【００４９】一般的なL2TPトンネルの場合のパケットのフォーマットは、図25に示す通りである。IPヘッダ、TCP/UDPヘッダ及びアプリケーションデータから成るパケットは、L2TPトンネルに送信される際にカプセル化に伴ってL2TPヘッダ及びPPPヘッダが付加される。さらにエッジルータがカプセル化されたパケットをプロバイダ網へ送信する際には下位メディアPPP/etherヘッダ等並びにIPヘッダ及びUDPヘッダが付加される。

【００５０】また、一般的なIPsecトンネルの場合は、認証機能を持つ認証ヘッダAH(authentication header)を使用する場合と、認証と暗号化の両機能を持つESP(encapsulating security payload)ヘッダを使用する場合があり、それぞれIPsecトンネル内を中継されるパケットのフォーマットは図26及び図27に示される。

【００５１】図26に示す如く、AHヘッダを使用したパケットでは、外側IPv4ヘッダ、AHヘッダ、内側IPv4ヘッダ、及びIP上位層データが認証の対象となる。また、図27に示す如くESPヘッダを使用したパケットは、外側IPv4ヘッダ、ESPヘッダ、内側IPv4ヘッダ、IP上位層データ、ESPトレイラ、及びESP認証ヘッダで構成される。この内、外側IPv4ヘッダ及びESP認証ヘッダを除いた範囲が認証の対象となり、さらにESPヘッダを除いた範囲が暗号化の対象となる。

【００５２】

【発明が解決しようとする課題】ID-VPNサービスを行うために、プロバイダ管理者は、ユーザネットワークが接続されるエッジルータのポートに対して、VPN番号、又はVPN-IDを割り当てる。そして、同一VPNに属する拠点間で通信を可能とするためには、これらが相互にグローバル網を経由するトンネルで接続されており、かつ、他のVPN番号、又はVPN-IDを持つ拠点間の通信と区別される必要がある。

【００５３】IETF RFC2547の方式では、各エッジルータが、各ポートと各ポートが属する仮想閉域網との対応関係を把握し同一仮想閉域網のポート間を仮想リンク(レベル2トンネル)で接続する必要がある。RFC2547の方式では、各エッジルータ間を接続するレベル1トンネルを用いて、各エッジルータ上のBGP経路制御プロセスを接続するBGPセッションを張る。エッジルータは、このBGPセッションを用いて全てのVPNの経路情報を多重化して交換する。エッジルータは、本経路情報を基に、どのポートとどのポートをレイヤ2トンネルで接続するかを決定する。

【００５４】BGPプロトコルを用いて経路情報を配布するエッジルータは、どのVPNの、どのサイトの経路情報をどの仮想ルータに配布するかを設定する。また、BGPプロトコルにより経路情報を受信したエッジルータは、どのサイトから受信した経路を自身の仮想ルータへ格納するかを、プロバイダ管理者が、各エッジルータに手動設定する。このため、VPNの構成が複雑であったり、VPN数が増加すると、設定が非常に煩雑となる。

【００５５】また、一般にBGPはトランジットネットワークとなるプロバイダが主に利用する経路制御プロトコルであり、OSPF(open shortest path first)で経路制御を行っているプロバイダも少なくない。従って、VPN実現のためにプロバイダの全エッジルータでBGPを動かすことは大きなハードルとなっている。

【００５６】一方、draft-mushukrishnan-corevpn-arch-00.txtの方式では、同一VPNに属する(同一VPN-IDを持つ)各仮想ルータをレベル2トンネルで接続し、あるVPNに属するサイトさら受信した経路情報は、このVPNに属する仮想ルータを接続するレベル2トンネルを使用して仮想ルータ間で交換する。

【００５７】本方式は、MPLSをベースに提案されており、MPLSネットワーク内でMPLSトンネルであるLabel Switching Path(LSP)を生成するためにLabel Distribution Protocol (LDP)を利用しているため、IPトンネル(L2TP,IPsec)を用いた手法には応用できない。

【００５８】従って、本発明は、公衆データ通信網内の仮想閉域網構築方法及び装置並びに中継装置において、VPNを実現するために、RFC2547のような各VPNの経路情報を制御するための複雑な設定を行わずに、draft-mushukrishnan-corevpn-arch-00.txtで示したように、経路情報の交換を同一VPN内に属する仮想ルータ間を接続したトンネルを用いた行う場合において、各エッジルータ上の同一VPNに属する仮想ルータを発見し、同一VPNに属

する仮想ルータ同士をLSP以外のトンネル(L2TP,IPsec等)でも接続可能とすることを目的とする。

【００５９】

【課題を解決するための手段】上記の目的を達成するため、本発明に係る仮想閉域網構築方法は、公衆データ通信網内で仮想閉域網を終端する各中継装置が仮想閉域網毎に予め定められたマルチキャストアドレスを設定した制御パケットを生成してマルチキャストし、該マルチキャストアドレスに属する各中継装置が、該制御パケットを受信したとき、該制御パケットの送信元の中継装置への仮想リンクを生成し、該仮想リンクを介して応答パケットを返送し、以て該マルチキャストアドレスに属する全ての中継装置間に仮想リンクが生成されて該仮想閉域網が構築されることを特徴としている。

【００６０】すなわち、仮想通信網を終端する中継装置は、まず、仮想閉域網毎に予め定めておいたマルチキャストアドレスを設定した制御パケットを生成し、これを該アドレスへマルチキャストする。そして、該マルチキャストアドレスに属する中継装置は、該制御パケットの受信を契機に、該制御パケットの送信元の中継装置への仮想リンクを生成し、該仮想リンクを介して応答パケットを返送する。

【００６１】返送された応答パケットを受信した制御パケットの送信元の中継装置は、各仮想リンクがどの中継装置との間に生成されたものであるかを知ることが可能となる。このような動作を各中継装置が行うことによって、該マルチキャストアドレスに属する全ての中継装置間に仮想リンクが生成されるので該仮想閉域網を構築することができる。

【００６２】従って、公衆データ通信網内で仮想閉域網を終端する各中継装置は、各仮想閉域網とマルチキャストアドレスとの対応関係を把握していればよく、従来のRFC2547の方式(該中継装置の各ポートと各ポートが属する仮想閉域網との対応関係を把握し同一仮想閉域網のポート間を仮想リンクで接続する)に比べて、管理が簡素化される。

【００６３】また、仮想リンクの生成には種々の既存のトンネル技術を使用することができ、従来技術のようにMPLSトンネルの技術に限定されない。この場合、該中継装置は、受信した該制御パケットの認証を行ってもよい。これにより、マルチキャストで送信された制御パケットを善意の第三者以外が受信することに伴って起こり得る問題を回避することができる。

【００６４】本発明に係る仮想閉域網構築方法において生成される仮想リンクは、IPトンネル又はMPLSトンネルとすることができる。また、本発明に係る仮想閉域網構築装置は、公衆データ通信網内に仮想閉域網の構築を開始するときに、予め定められたマルチキャストアドレスを設定した該制御パケットを生成してマルチキャストする中継装置と、該制御パケットを受信したとき、該制御パケットの送信元との間に仮想リンクを生成し、該仮想リンクを介して応答パケットを返送する中継装置とを備え、各中継装置が作動して該マルチキャストアドレスに属する全ての中継装置間に仮想リンクが生成されることにより該仮想閉域網を構築することを特徴としている。

【００６５】すなわち、本発明に係る仮想閉域網構築装置は、公衆データ通信網内に仮想閉域網の構築を開始するときに、まず、或る中継装置が仮想閉域網毎に予め定められたマルチキャストアドレスを設定した制御パケットを生成してマルチキャストする。

【００６６】該制御パケットを受信した別の中継装置はこれを契機に、該制御パケットの送信元の中継装置への仮想リンクを生成し、該仮想リンクを介して応答パケットを返送する。制御パケットの送信元の中継装置は、返送された応答パケットを受信することにより、各仮想リンクがどの中継装置との間に生成されたものであるかを知ることが可能となる。

【００６７】各中継装置がこのように作動すれば該マルチキャストアドレスに属する全ての中継装置間に仮想リンクが生成され、該仮想閉域網を構築することができる。従って、この仮想閉域網構築装置においても、仮想閉域網構築方法と同様に、従来のRFC2547の方式に比べて管理が簡素化されると共にMPLSトンネルの技術に限定されない。

【００６８】この場合、該仮想リンクを生成する中継装置が、受信した該制御パケットの認証を行ってもよい。これにより、マルチキャストで送信された制御パケットを善意の第三者以外が受信することに伴って起こり得る問題を回避することができる。

【００６９】本発明に係る仮想閉域網構築装置によって生成される仮想リンクはIPトンネル又はMPLSトンネルとすることができる。また、本発明に係る中継装置は、公衆データ通信網内で仮想閉域網を終端する中継装置において、仮想閉域網毎に予め定められたマルチキャストアドレスを設定した該制御パケットを生成してマルチキャストする手段と、該制御パケットを受信したとき、該制御パケットの送信元の該中継装置との間に仮想リンクを生成し、該仮想リンクを介して応答パケットを返送する手段と、を備え、以て該マルチキャストアドレスに属する全ての中継装置間に仮想リンクを生成することにより該仮想閉域網を構築することを特徴としている。

【００７０】すなわち、本発明に係る中継装置は、仮想閉域網毎に予め定められたマルチキャストアドレスを設定した制御パケットを生成してマルチキャストし、該制御パケットを受信したとき、該制御パケットの送信元の中継装置への仮想リンクを生成し、該仮想リンクを介して応答パケットを返送する。

【００７１】制御パケットの送信元の中継装置は、返送された応答パケットを受信することにより、各仮想リンクがどの中継装置との間に生成されたものであるかを知

ることが可能となる。公衆データ通信網内で仮想閉域網を終端する各中継装置がこのように作動すれば該マルチキャストアドレスに属する全ての中継装置間に仮想リンクが生成され、該仮想閉域網を構築することができる。

【００７２】従って、この中継装置を使用すれば、公衆データ通信網内で仮想閉域網を構築する際、従来のRFC2547の方式に比べて管理が簡素化されると共にMPLSトンネルの技術に限定されない。また、本発明に係る中継装置は、受信した該制御パケットの認証を行う手段をさらに備えてもよい。

【００７３】これにより、マルチキャストで送信された制御パケットを善意の第三者以外が受信することに伴って起こり得る問題を回避することができる。さらに、本発明に係る中継装置は、論理的に互いに独立した複数の仮想閉域網それぞれの経路表を生成する手段と、該経路表に基づいて各仮想閉域網のパケット中継を行う手段とをさらに備えてもよい。

【００７４】すなわち、論理的に互いに独立した複数の仮想閉域網それぞれについて経路表が生成され、各仮想閉域網のパケット中継が該経路情報に基づいて行われる。従って、この場合のパケット中継は、各仮想閉域網で論理的に独立して行われることになる。

【００７５】これにより、異なる仮想閉域網間の混乱を生じることなく、各仮想閉域網において論理的に独立したパケット中継を行うことが可能となる。本発明に係る中継装置によって生成される仮想リンクはIPトンネル又はMPLSトンネルとすることができる。

【００７６】

【発明の実施の形態】本発明の実施例を図1を用いて説明する。この実施例は、図23と同様な構成を有するが、ユーザネットワークUN2にIPアドレス[private1.2.23]を有するホストが接続され、ユーザネットワークUN5にはIPアドレス[private1.5.25]を有するサーバが接続されている。

【００７７】また、詳細な説明を行うため、各物理ポート、各仮想インタフェース、各ネットワーク、及び各トンネルにそれぞれ対応する主なIPアドレスが大括弧[]内に示されている。"lo0"で始まるインタフェースは、ループバックインタフェースと呼ばれ、いずれの物理的／論理的リンクにも接続されていない仮想的なインタフェースである。これらのインタフェースのアドレスは、しばしばルータを代表するものとして使用される。

【００７８】なお、IPアドレスは、IPv4では4バイトの整数を1バイトづつ区切って表記される(168.254.192.0等)が、本実施例では、上位2バイト又は3バイトをprivate1やglobal等の文字列として置き換えて表記する。また、アドレス表記としてIPアドレスの最後が"/24"であるものは、マスクビットが24ビットであることを示しており、主としてIPアドレスにおけるネットワークのIPアドレスを示すビット長を表現するのに用いられる。

【００７９】なお、図2は図1のVPN1内に存在する各仮想ルータの各仮想インタフェースに割り振られたIPアドレスを示したものであり、例えば、仮想インタフェースVR1-VP2にはIPアドレス[private1.20.1]が対応付けられている。また、図3は図1のエッジルータPR1,PR4,及びPR5の各インタフェースに割り振られたIPアドレスを示したものであり、例えばインタフェースPR1-PP1にはIPアドレス[private2.10.1]が対応付けられている。

【００８０】さらに、図4は図１の各ユーザルータUR1～UR6のインタフェースに割り振られたIPアドレスを示したものであり、例えば、インタフェースUR1-PP1にはIPアドレス[private2.10.2]が対応付けられている。まず、本実施例における仮想閉域網の構築手順について、エッジルータPR1及びPR4で行われる手順を例に説明する。

【００８１】図5は、図1に示したISPネットワークNW1内のエッジルータPR1及びPR4の装置内の構成を示したものであるが、説明の便宜上、エッジルータPR1及びPR4をISPネットワークNW1の外に示している。両エッジルータPR1及びPR4は同じ構成を有するものであり、それぞれ手段としては、パケット送信手段101、パケット受信手段102、イニシエーションパケット送信手段201、応答パケット送信手段202、仮想リンク生成手段203、イニシエーションパケット受信手段204、及び応答パケット受信手段205を備えている。

【００８２】さらに、テーブルとして、VPN-ID-仮想ルータ対応テーブル301、VPN-ID-マルチキャストアドレス対応テーブル302、仮想インタフェース管理テーブル303、プライベートアドレス解決テーブル304、及びVPN多重化テーブル305を有している。

【００８３】なお、ネットワークNW1内で共通になるように、VPN毎のVPN-ID及び各VPN-IDに対応したマルチキャストアドレスがプロバイダ網管理者によって予め定められているものとする。今、図1におけるVPN1及びVPN2のVPN-IDがそれぞれ"1"及び"2"であるとすると、図5におけるエッジルータPR1内のVPN-ID-仮想ルータ対応テーブル301は、図6(1)に示すように、例えばVPN-ID=1に対して仮想ルータVPN1-VR1が対応するように設定される。同様に、図6(2)にはエッジルータPR4内のVPN-ID-仮想ルータ対応テーブル301の例が示されている。

【００８４】また、VPN-ID-マルチキャストアドレス対応テーブル302は、ネットワークNW1内で共通となるため、エッジルータPR1及びPR4で同じ内容となる。図7は、VPN-ID-マルチキャストアドレス対応テーブル302の例を示したものであり、例えばVPN-ID=1に対してマルチキャストアドレス[239.192.0.1]が対応するように設定されている。

【００８５】さらに、図1におけるネットワークNW1内の全ルータPR1～PR5は、グローバルアドレス空間においてマルチキャストルーティングプロトコルを起動し、マル

チキャストパケットの配信が可能な状態になっているものとする。トンネル技術として、L2TP，IPsecといったプロトコルを用いることが可能であるが、この実施例ではトンネル技術としてL2TPを用いた場合について、エッジルータPR1及びPR4が同一VPNに属する仮想ルータ間に自動的にトンネルを生成する手順を説明する。

【００８６】(1)図5において、まず、エッジルータPR1のイニシエーションパケット送信手段201は、VPN-ID-仮想ルータ対応テーブル301を参照し、設定されているVPN-ID毎に制御パケットであるトンネルイニシエーションメッセージ(以降、イニシエーションメッセージと称する。)を生成した後、VPN-ID-マルチキャストアドレス対応テーブル302を参照し、VPN-IDに対応するマルチキャストアドレスを宛先アドレスとして設定したイニシエーションメッセージをパケット送信手段101を介してネットワークNW1へ送信する。

【００８７】イニシエーションメッセージのパケットフォーマットは図8に示す通りであるが、例えば、VPN-ID=1に対応するイニシエーションメッセージのフィールド値は図9に示すようになる。

(2)エッジルータPR4では、パケット受信手段102を介してイニシエーションパケット受信手段204が上記イニシエーションメッセージを受信すると、仮想リンク生成手段203を用いて、イニシエーションメッセージ中のSRC IPアドレス（この場合は、エッジルータPR1のIPアドレス）へ向けてトンネルを生成する。

【００８８】このとき、イニシエーションメッセージ中の"トンネルタイプ"フィールドの値が"0"、すなわちL2TPトンネルを示しているため、L2TPトンネルが生成される。これにより、エッジルータPR4では、L2TPトンネルのトンネルIDとセッションIDを得る。L2TPトンネルの場合、イニシエーションメッセージを受信したエッジルータからの応答方向を上り方向とし、その逆を下り方向とすると、両方向のトンネルが同時に生成される。

【００８９】従って、ここでは、上り(PR4→PR1)、下り(PR1→PR4)の各トンネルに対して例えば図10(1)及び(2)に示すようなトンネルID及びセッションIDの値がそれぞれ得られる。次に、メッセージ内のVPN-IDに対応する仮想ルータVPN1-VR2が、新たな仮想インタフェース(図1のV1-VR2-VP1)を生成し、この仮想インタフェースV1-VR2-VP1と接続先アドレス(イニシエーションメッセージのSRC IP)の対応を仮想インタフェース管理テーブル303に登録する。

【００９０】また、生成した仮想インタフェースV1-VR2-VP1と上りトンネルのトンネルID、セッションIDの対応をVPN多重化テーブル305に登録する。さらに、イニシエーションメッセージのIPヘッダに含まれるイニシエーションメッセージの送信元であるエッジルータPR1のIPアドレス(この例では、PR1-PP6のIPアドレス)と、イニシエーションメッセージのSRC IPフィールドに含まれる送信元仮想ルータVPN1-VR1のIPアドレスの対応を、プライベートアドレス解決テーブル304に登録する。

【００９１】(3)次に、エッジルータPR4は、生成したトンネルを介して、応答メッセージを送信する。応答メッセージのパケットフォーマットは図8に示したイニシエーションメッセージのフォーマットと同じであり、この場合の応答メッセージの各フィールドの値は図11のようになる。

【００９２】(4)上記の応答メッセージを受信したエッジルータPR1は、応答メッセージ中のVPN-IDに対応する仮想ルータVPN1-VR1に対し、新たな仮想インタフェースV1-VR1-VP6を新たに生成する。その後、仮想ルータ、仮想インタフェース、応答メッセージ中のトンネルID,セッションIDの対応を後述する逆多重化テーブルに設定する。本テーブルは、エッジルータPR1がL2TPトンネルから応答パケットを受信した際に、セッションID及びトンネルIDの値からどの仮想ルータのどの仮想インタフェースでパケットを受信するかを決定するために参照するテーブルである。

【００９３】上記(1)～(4)の処理手順は、エッジルータPR4からイニシエーションメッセージを送信する場合にも同様にして行われる。以上、図5を用いた説明では、2つのエッジルータPR1及びPR4間の処理を説明したが、実際には多くのエッジルータが存在しており、図1に示す如くエッジルータが3つある場合には、例えばエッジルータPR1からマルチキャストされるイニシエーションメッセージは、VPN1に関してはVPN1のマルチキャストアドレスに属するエッジルータPR4及びPR5によって受信され、VPN2に関してはVPN2のマルチキャストアドレスに属するエッジルータPR4のみによって受信されるようになる。

【００９４】このような動作をネットワークNW1内の全てのエッジルータが相互に行なえば、複数のVPNについて同一VPNに含まれる仮想ルータ間でL2TPトンネルをフルメッシュに生成することができる。なお、図12は、図5における各エッジルータPR1及びPR4内に制御パケット認証手段103及び認証データベース104を設ける場合のイニシエーションパケット受信手段204及び応答パケット受信手段205との接続例を示したものである。

【００９５】この場合、プロバイダが管理するエッジルータで共通のパスワードを各エッジルータの認証データベース104に登録しておく。そして、動作においては、イニシエーションパケット受信手段204は、制御パケット認証手段104を用いて受信したイニシエーションパケットのパスワードを制御パケット認証手段104に登録されたパスワードとして認証できた場合のみ、エッジルータPR1からイニシエーションメッセージを受信することになる。

【００９６】また、応答パケット受信手段205は、制御パケット認証手段103を用いて、受信したイニシエーシ

ョンパケットのパスワードを制御パケット認証手段104に登録されたパスワードとして認証できた場合のみ応答パケットを受信する。このようにしてトンネルをフルメッシュに生成して構築されたVPNにおいて、実際に各エッジルータが行うパケット中継の処理手順について以下に説明する。

【００９７】VPNを実現するプロバイダ網内の通信は、以下に示す二段階の通信に分けて考えることができる。

(1)バックボーンネットワークの通信

(2)オーバレイネットワークの通信

バックボーンネットワークの通信(1)は、グローバルアドレスを用いる通信であり、プロバイダ網が管理するインターネット経路情報に基づき、プロバイダ網内のインターネット経路情報を保持する(物理)ルータ、及びルータ間を接続する物理的／論理的なリンクにより実現される。

【００９８】オーバレイネットワークの通信(2)は、プライベートアドレスを用いる通信であり、ユーザが持つイントラネット経路情報に基づき、ユーザ経路情報を管理する仮想ルータと、バックボーンネットワーク上に仮想的に生成された仮想ルータ間を接続するトンネルにより実現される。オーバレイネットワークの通信は、実際には、バックボーンネットワークの通信パケットとしてカプセル化され、バックボーンネットワークを転送される。

【００９９】このようなバックボーンネットワークの通信(1)及びオーバレイネットワークの通信(2)を実現する各エッジルータが行うパケット中継処理を説明するため、図13は、図5に示した、エッジルータPR1及びPR4について共通となるように示したエッジルータの構成をさらに詳細に示したものである。

【０１００】図13の実施例では、図5に示したエッジルータの構成に加えて、パケット中継処理に関連する手段として、パケット種別判定手段501、パケット逆多重化手段502、仮想ルータ検索手段503、パケットカプセル化手段504、グローバル経路制御手段505、及びユーザ経路制御手段506をさらに備えている。

【０１０１】さらに、仮想ルータ経路表401、ユーザ収容I/F-VPN対応テーブル402、逆多重化テーブル403、及びグローバルインターネット経路表404が示されている。以下、図1におけるエッジルータPR1が図13に示した構成を有するものとしてエッジルータPR1のパケット中継処理手順を説明する。なお、図13の構成についても、図5の場合と同様に図12に示す制御パケット認証手段103及び認証データベース104を設けてもよいが、ここでは説明を省略する。

【０１０２】グローバル経路制御手段505は、インターネットにおける、他ルータ上のグローバル経路制御手段505とグローバルアドレス経路情報を交換し、グローバルインターネット経路表404を生成する。図14は、エッジルータPR1におけるグローバルインターネット経路表404の例を示したものである。図1に示すように、アドレス[global1.0/24]は、エッジルータPR1とコアルータPR2を結ぶネットワークに割り当てられたIPアドレスである。

【０１０３】従って、図14においては、アドレス[global1.0/24]は、次ホップ="直接"、出力ポート=PR1-PP6に対応付けられている。また、エッジルータPR1におけるユーザ経路制御手段506は、ネットワークNW1における他のエッジルータPR4及びPR5上のユーザ経路制御手段506と、ユーザネットワークUN1及びUN2におけるユーザルータUR1及びUR2上のユーザ経路制御手段との間でプライベートアドレスで表示されるユーザ経路情報を交換して、仮想ルータ毎の仮想ルータ経路表401を生成する。

【０１０４】図15は、エッジルータPR1における仮想ルータ経路表401の例として、仮想ルータVPN1-VR1の仮想ルータ経路表を示したものである。例えば、宛先をアドレス[private1.6.0/24]とする経路は、同図に示す如く次ホップ=[private1.100.3]、出力仮想I/F=V1-VR1-VP5に対応付けられている。

【０１０５】これは、図1の仮想ルータVPN1-VR1からアドレス[private1.6.0/24]を有するユーザネットワークUR6への経路として、アドレス[private1.100.3]を有する仮想ルータVPN1-VR3を経由し、この場合の出力仮想I/FがV1-VR1-VP5であることを示している。

【０１０６】このときのエッジルータPR1のユーザ収容インタフェース-仮想ルータ対応テーブル402の例を図16に示す。この場合、例えば物理インタフェースPR1-PP1にはVPN-ID=2、仮想ルータ=VPN2-VR1、及び仮想インタフェースV2-VR1-VP1が対応付けられている。

【０１０７】また、VPN1-VR1の仮想インタフェース管理テーブル303の例を図17に示す。この場合、例えば仮想インタフェースV1-VR1-VP2には自アドレスとして[private1.2.1]、接続先アドレスとして[private1.20.2]、カプセル化="する"、出力ポートPR1-PP2が対応付けられている。カプセル化フィールドは、カプセル化をするか否かを示すフィールドであり、この場合、仮想インタフェースV1-VR1-VP2にはユーザネットワークUN2のユーザルータUR2が接続されているため、カプセル化は行わない。

【０１０８】同図において、例えば仮想インタフェースV1-VR1-VP5に関しては、L2TPトンネルを介してアドレス[private1.100.3]を有する仮想ルータVPN1-VR3に接続されているのでカプセル化フィールドは、"する"となっている。また、プライベートアドレス解決テーブル304の例を図18に示す。プライベートアドレス解決テーブルは、宛先仮想ルータのIPアドレスから、宛先仮想ルータが存在するエッジルータのグローバルなIPアドレスを取得するためのテーブルである。仮想ルータへパケットを送信する際、実際には、仮想ルータ宛のパケットをグロ

ーバルアドレスを持つパケットでカプセル化し、エッジルータへ送るため、エッジルータのグローバルなIPアドレスが必要となる。この場合、例えばプライベートアドレス[private1.100.2]がグローバルアドレス[global3.2]に対応付けられている。

【０１０９】さらに、VPN多重化テーブル305の例を図19に示す。VPN多重テーブルは、宛先仮想ルータへパケットを送信する際、アドレスによりどのIPトンネルへパケットを送信するかを記述したテーブルである。この場合、たとえば接続先仮想ルータアドレス［private1.100.2]には送信トンネルID＝300、送信セッションID=202が対応付けられている。

【０１１０】ここで、図1におけるアドレス[private2.0/24]を有するユーザネットワークUN2内のホスト[private1.2.23]から、アドレス[private1.5.0/24]を有するユーザネットワークUN5内のサーバ[private1.5.25]にアクセスする場合を想定する。ユーザネットワークUN2からエッジルータPR1のポートPR1−PP2にパケットが到着すると、エッジルータPR1は、パケットを受信したポート番号(PR1−PP2)からユーザ収容インタフェース−仮想ルータ対応テーブル402(図16)を参照し、ユーザネットワークUN2が属するVPNのVPN−ID=1及び仮想ルータVPN1−VR1を特定し、受信したパケットを仮想ルータに渡す。

【０１１１】パケットを受信した仮想ルータVPN1−VR1は、VPN1に属するユーザネットワークの経路情報を含む仮想ルータ経路表401(図15)を参照し、宛先ユーザネットワーク[private1.5.0/24]に対応付けられた次ホップ仮想ルータVPN1−VR2のアドレスNext Hop=[private1.100.2]及び出力仮想I/FであるV1−VR1−VP6を得る。

【０１１２】仮想ルータVPN1−VR1は、次ホップ仮想ルータVPN1−VR2が接続される仮想インタフェースV1−VR1−VP6へパケットを送信する。このとき、エッジルータPR1は、VPN多重化テーブル305(図19)を参照し、パケットをL2TPカプセル化する。この例では、VPN多重化テーブル305の[private1.100.2]のエントリがヒットし、送信トンネルID=300及び送信セッションID=202を得る。

【０１１３】また、プライベートアドレス解決テーブル304(図18)を検索し、次ホップ仮想ルータVPN1−VR2のアドレス[private1.100.2]から、次ホップエッジルータPR4のグローバルアドレス[global3.2]を決定する。エッジルータPR1では、ユーザネットワークUN2から受信したパケットをL2TPカプセリングし、宛先IPアドレスを先に求めたグローバルアドレス[global3.2]としたIPヘッダを付加した上で、グローバルインターネット経路表404(図14)を検索し、出力ポートに示されるインタフェースPR1−PP6にカプセル化したパケットを送信する。

【０１１４】逆に、サーバ[private1.5.25]からホスト[private1.2.23]に応答が返って来た場合の動作を以下に説明する。エッジルータPR1は、物理インタフェースPR1−PP6からL2TPカプセル化された応答パケットを受信した場合、カプセルヘッダ内のトンネルIDとセッションIDをキーとして、VPN逆多重化テーブル403を参照する。

【０１１５】この場合のエッジルータPR1におけるVPN逆多重化テーブル403の例を図20に示す。このテーブルは、エッジルータPR1がL2TPトンネルからパケットを受信した際に、セッションID及びトンネルIDの値に基づき、どの仮想ルータのどの仮想インタフェースでパケットを受信するかを決定するために参照するテーブルである。

【０１１６】例えば、同図に示す如く、受信トンネルID=105、受信セッションID=200のパケットを受信した場合は、仮想ルータVPN1−VR1の仮想インタフェースV1−VR1−VP6で受信することが分かる。この時、エッジルータPR1は、カプセルヘッダを外して受信パケットを仮想ルータVPN1−VR1に渡す。仮想インタフェースV1−VR1−VP6でパケットを受信した仮想ルータVPN1−VR1は、受信したIPパケット(L2TPヘッダが外れた後のプライベートアドレスを持つIPパケット)のIPヘッダの宛先アドレス（これはユーザネットワーク内の宛先アドレスである）を見て、仮想ルータVPN1−VR1の仮想ルータの経路表401(図15)を検索する。

【０１１７】この場合、宛先アドレスが[private1.2.0/24]のエントリにヒットすることからパケットを仮想インタフェースV1−VR1−VP2に送信すればよいことが分かる。そこで、エッジルータPR1は、仮想インタフェース管理テーブル303(図17)を参照し、仮想インタフェースV1−VR1−VP2に対応付けられた出力ポートPR1−PP2へパケットを送信する。このとき、同テーブルのカプセル化フィールドが"しない"であることから、カプセル化は行わない。

【０１１８】なお、本実施例においては、トンネル技術としてL2TPトンネルを用いる場合について説明した。この場合、L2TPトンネル内を通るカプセル化されたパケットのフォーマットは、図25に示す通りである。但し、本発明ではトンネル技術を限定していないため、IPsecトンネルを用いてもよく、また、MPLSトンネルを用いることも可能である。

【０１１９】（付記１）公衆データ通信網内で仮想閉域網を終端する各中継装置が仮想閉域網毎に予め定められたマルチキャストアドレスを設定した制御パケットを生成してマルチキャストし、該マルチキャストアドレスに属する各中継装置が、該制御パケットを受信したとき、該制御パケットの送信元の中継装置への仮想リンクを生成し、該仮想リンクを介して応答パケットを返送し、以て該マルチキャストアドレスに属する全ての中継装置間に仮想リンクが生成されて該仮想閉域網が構築されることを特徴とする仮想閉域網構築方法。

【０１２０】（付記２）付記１において、該中継装置が受信した該制御パケットの認証を行うことを特徴とする仮想閉塞網構築方法。

（付記３）付記１において、該仮想リンクがIPトンネルであることを特徴とした仮想閉域網構築方法。

【０１２１】（付記４）付記１において、該仮想リンクがMPLSトンネルであることを特徴とした仮想閉域網構築方法。

（付記５）公衆データ通信網内に仮想閉域網の構築を開始するときに、予め定められたマルチキャストアドレスを設定した該制御パケットを生成してマルチキャストする中継装置と、該制御パケットを受信したとき、該制御パケットの送信元との間に仮想リンクを生成し、該仮想リンクを介して応答パケットを返送する中継装置とを備え、各中継装置が作動して該マルチキャストアドレスに属する全ての中継装置間に仮想リンクが生成されることにより該仮想閉域網を構築することを特徴とした仮想閉域網構築装置。

【０１２２】（付記６）付記５において、該仮想リンクを生成する中継装置が、受信した該制御パケットの認証を行うことを特徴とする仮想閉域網構築装置。

（付記７）付記５において、該仮想リンクがIPトンネルであることを特徴とした仮想閉域網構築装置。

【０１２３】（付記８）付記５において、該仮想リンクがMPLSトンネルであることを特徴とした仮想閉域網構築装置。

（付記９）公衆データ通信網内で仮想閉域網を終端する中継装置において、仮想閉域網毎に予め定められたマルチキャストアドレスを設定した該制御パケットを生成してマルチキャストする手段と、該制御パケットを受信したとき、該制御パケットの送信元の該中継装置との間に仮想リンクを生成し、該仮想リンクを介して応答パケットを返送する手段と、を備え、以て該マルチキャストアドレスに属する全ての中継装置間に仮想リンクを生成することにより該仮想閉域網を構築することを特徴とする中継装置。

【０１２４】（付記１０）付記９において、受信した該制御パケットの認証を行う手段をさらに備えたことを特徴とする中継装置。

（付記１１）付記９において、論理的に互いに独立した複数の仮想閉域網それぞれの経路表を生成する手段と、該経路表に基づいて各仮想閉域網のパケット中継を行う手段とをさらに備えたことを特徴とする中継装置。

【０１２５】（付記１２）付記９において、該仮想リンクがIPトンネルであることを特徴とした中継装置。

（付記１３）付記９において、該仮想リンクがMPLSトンネルであることを特徴とした中継装置。

【０１２６】

【発明の効果】以上説明したように、本発明に係る仮想閉域網構築方法及び装置並びに中継装置は、マルチキャストアドレスを設定した制御パケットが生成されてマルチキャストされ、該制御パケットが該マルチキャストアドレスに属する中継装置によって受信されると、該制御パケットの送信元の中継装置への仮想リンクが生成され、該仮想リンクを介して応答パケットが返送され、以て該マルチキャストアドレスに属する全ての中継装置間に仮想リンクが生成されることにより仮想閉域網を構築するように構成したので、複雑なVPN管理が不要で且つ種々のトンネル技術に適用可能にすることができる。

【図面の簡単な説明】

【図１】本発明の実施例を説明するためのネットワーク図である。

【図２】図1における仮想インタフェースに割り振られたIPアドレスの実施例を示した図である。

【図３】図1におけるエッジルータの各インタフェースに割り振られたIPアドレスの実施例を示した図である。

【図４】図1におけるユーザルータの各インタフェースに割り振られたIPアドレスの実施例を示した図である。

【図５】図1におけるエッジルータの動作を説明するためのブロック図である。

【図６】本発明に係るVPN-ID-仮想ルータ対応テーブルの実施例を示した図である。

【図７】本発明に係るVPN-ID-マルチキャストアドレス対応テーブルの実施例を示した図である。

【図８】本発明に係るトンネルイニシエーションメッセージのパケットフォーマットを示した図である。

【図９】図8のフィールド値の実施例を示した図である。

【図10】本発明に係るトンネルID及びセッションIDの設定例を示した図である。

【図11】本発明に係る応答メッセージのフィールド値の実施例を示した図である。

【図12】図5の構成に追加可能な手段の接続例を示したブロック図である。

【図13】図1におけるエッジルータの詳細構成例を示したブロック図である。

【図14】本発明に係るグローバルインターネット経路表の実施例を示した図である。

【図15】本発明に係る仮想ルータ経路表の実施例を示した図である。

【図16】本発明に係るユーザ収容インタフェース-仮想ルータ対応テーブルの実施例を示した図である。

【図17】本発明に係る仮想インタフェース管理テーブルの実施例を示した図である。

【図18】本発明に係るプライベートアドレス解決テーブルの実施例を示した図である。

【図19】本発明に係るVPN多重化テーブルの実施例を示した図である。

【図20】本発明に係るVPN逆多重化テーブルの例を示した図である。

【図21】一般的なVPNのグローバルインターネットへのオーバレイを示したネットワーク図である。

【図22】従来のVPN構成例(1)を示したネットワーク図で

ある。

【図23】従来のVPN構成例(2)を示したネットワーク図である。

【図24】従来のVPN構成例(1)及び(2)におけるMPLSトンネル内のパケットフォーマットを示した図である。

【図25】一般的なL2TPトンネル内のパケットフォーマットを示した図である。

【図26】一般的なIPsecトンネル内のAHヘッダを用いた場合のパケットフォーマットを示した図である。

【図27】一般的なIPsecトンネル内のESPヘッダを用いた場合のパケットフォーマットを示した図である。

【符号の説明】

101　パケット送信手段
102　パケット受信手段
103　制御パケット認証手段
104　認証データベース
201　イニシエーションパケット送信手段
202　応答パケット送信手段
203　仮想リンク生成手段
204　イニシエーションパケット受信手段
205　応答パケット受信手段
301　VPN-ID-仮想ルータ対応テーブル
302　VPN-ID-マルチキャストアドレス対応テーブル
＊303　仮想インタフェース管理テーブル
304　プライベートアドレス解決テーブル
305　VPN多重化テーブル
401　仮想ルータ経路表
402　ユーザ収容インタフェース-仮想ルータ対応表
403　VPN逆多重化テーブル
404　グローバルインターネット経路表
501　パケット種別判定手段
502　パケット逆多重化手段
503　仮想ルータ検索手段
504　パケットカプセル化手段
505　グローバル経路制御手段
506　ユーザ経路制御手段
NW1　IPSネットワーク
PR1，PR4，PR5　エッジルータ
PR2，PR3　コアルータ
UN1～UN6　ユーザネットワーク
UR1～UR6　ユーザルータ
VPN1，VPN2　仮想閉域網
VPN1-VR1，VPN1-VR2，VPN2-VR1，VPN1-VR2　仮想ルータ
V1-VR1-VP2～V2-VR2-VP6　仮想インタフェース
PR1-PP1～PR5-PP8　物理インタフェース（ポート）
＊　図中、同一符号は同一又は相当部分を示す。

【図２】

仮想インタフェースに割り振られたIPアドレス

仮想インタフェース名	IPアドレス
V1-VR1-VP2	private1.20.1
V1-VR1-VP5	private1.11.1
V1-VR1-VP6	private1.10.1
V1-VR2-VP1	private1.10.2
V1-VR2-VP2	private1.12.2
V1-VR2-VP5	private1.30.1
V1-VR3-VP1	private1.11.2
V1-VR3-VP4	private1.12.1
V1-VR3-VP6	private1.40.1
lo0-VPN1-VR1	private1.100.1
lo0-VPN1-VR2	private1.100.2
lo0-VPN1-VR3	private1.100.3
lo0-VPN2-VR1	private2.100.1
lo0-VPN2-VR2	private2.100.2

【図３】

エッジルータの各インタフェースに割り振られたIPアドレス

インタフェース名	IPアドレス
PR1-PP1	private2.10.1
PR1-PP2	private1.20.1
PR1-PP6	global1.1
PR2-PP2	global1.2
PR4-PP3	global3.2
PR4-PP4	private2.30.1
PR4-PP5	private1.30.1
PR4-PP6	private2.50.1
PR5-PP2	global4.2
PR5-PP8	private1.40.1
lo0-PR1	global100.1
lo0-PR4	global100.2
lo0-PR5	global100.3

【図４】

ユーザルータの各インタフェースに割り振られたIPアドレス

インタフェース名	IPアドレス
UR1-PP1	private2.10.2
UR2-PP1	private1.20.2
UR3-PP1	private2.30.2
UR5-PP1	private2.50.2
UR6-PP1	private1.30.2
UR7-PP1	private1.40.2

【図７】

VPN-ID―マルチキャストアドレス対応テーブル

VPN-ID	マルチキャストアドレス
1	239.192.0.1
2	239.192.0.2
…	…
1024	239.192.4.0

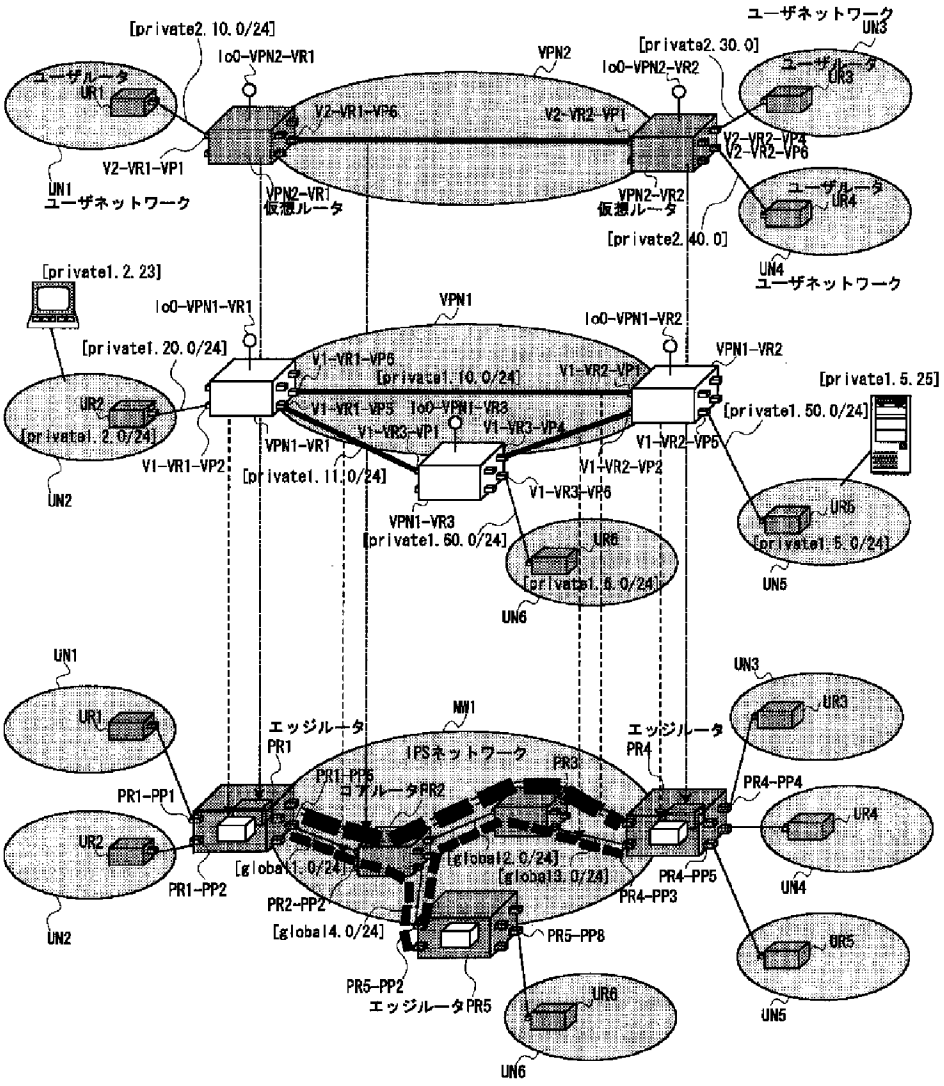
【図１６】

エッジルータPR1のユーザ収容インタフェース―仮想ルータ対応テーブル

物理インタフェース	VPN-ID	仮想ルータ	仮想インタフェース
PR1-PP1	2	VPN2-VR1	V2-VR1-VP1
PR1-PP2	1	VPN1-VR1	V1-VR1-VP2

【図１】

本発明の実施例



【図９】

トンネルイニシエーションメッセージのフィールド値

メッセージタイプ	0
VPN-ID	1
SRC IP アドレス	private1.100.1
トンネルタイプ	0(L2TP)
トンネルID	0
セッションID	0
パスワード	11111

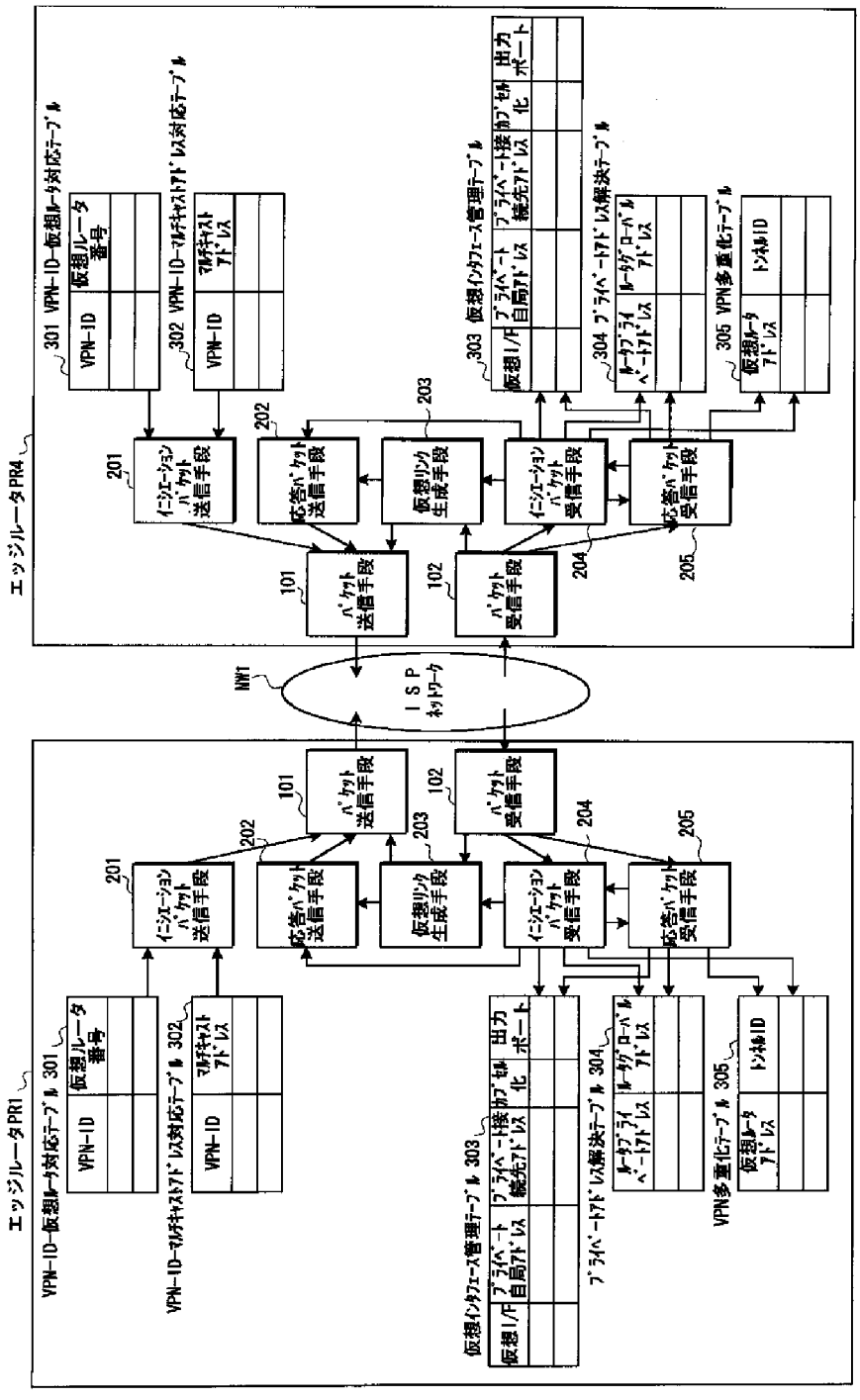
【図１１】

応答メッセージのフィールド値

メッセージタイプ	1
VPN-ID	1
SRC IP アドレス	private1.100.2
トンネルタイプ	0(L2TP)
トンネルID	105
セッションID	200
パスワード	11111

【図５】

図１におけるエッジルータの動作例



【図６】

VPN-ID--仮想ルータ対応表

（１） エッジルータ PR1

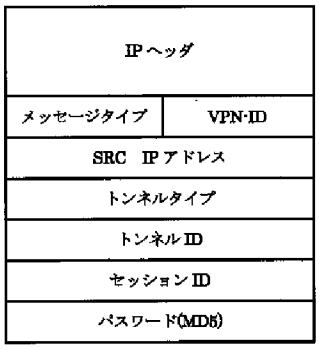
VPN-ID	仮想ルータ
1	VPN1-VR1
2	VPN2-VR1

（２） エッジルータ PR4

VPN-ID	仮想ルータ
1	VPN1-VR2
2	VPN2-VR2

【図８】

トンネルイニシエーションメッセージのパケットフォーマット



【図１０】

トンネル ID 及びセッション ID

（１） 上りトンネル（PR4→PR1）

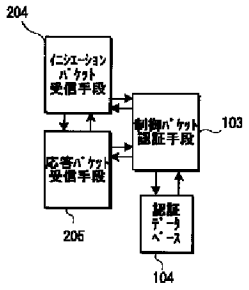
Tunnel ID	105
Session ID	200

（２） 下りトンネル（PR1→PR4）

Tunnel ID	300
Session ID	202

【図１２】

図５に追加可能な手段の接続例



【図１４】

エッジルータ PR1 のグローバルインタネット経路表

宛先	次ホップ	出力ポート
global1.0/24	Direct	PR1-PP6
global2.0/24	global1.2	PR1-PP6
global3.0/24	global1.2	PR1-PP6
global4.0/24	global1.2	PR1-PP6

【図１５】

仮想ルータ VPN1-VR1 の仮想ルータ経路表

宛先	次ホップ	出力仮想インタフェース
private1.6.0/24	private1.100.3	V1-VR1-VP5
private1.5.0/24	private1.100.2	V1-VR1-VP6
private1.2.0/24	private1.20.2	V1-VR1-VP2

【図１７】

VPN1-VR1 の仮想インタフェース管理テーブル

仮想インタフェース	自アドレス	接続先アドレス	カプセル化	出力ポート
V1-VR1-VP2	private1.2.1	private1.20.11	しない	PR1-PP2
V1-VR1-VP5	private1.10.1	Private1.100.3	する	--
V1-VR1-VP6	private1.11.1	Private1.100.2	する	--

【図１８】

エッジルータ PR1 のプライベートアドレス解決テーブル

プライベートアドレス	グローバルアドレス
private1.100.2	global3.2
Private2.100.2	global3.2
Private1.100.3	global4.2

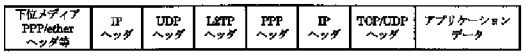
【図１９】

エッジルータ PR1 の VPN 多重化テーブル

接続先仮想ルータアドレス	送信トンネル ID	送信セッション ID
private1.100.2	300	202
private1.100.3	301	243
private2.100.2	1001	1201

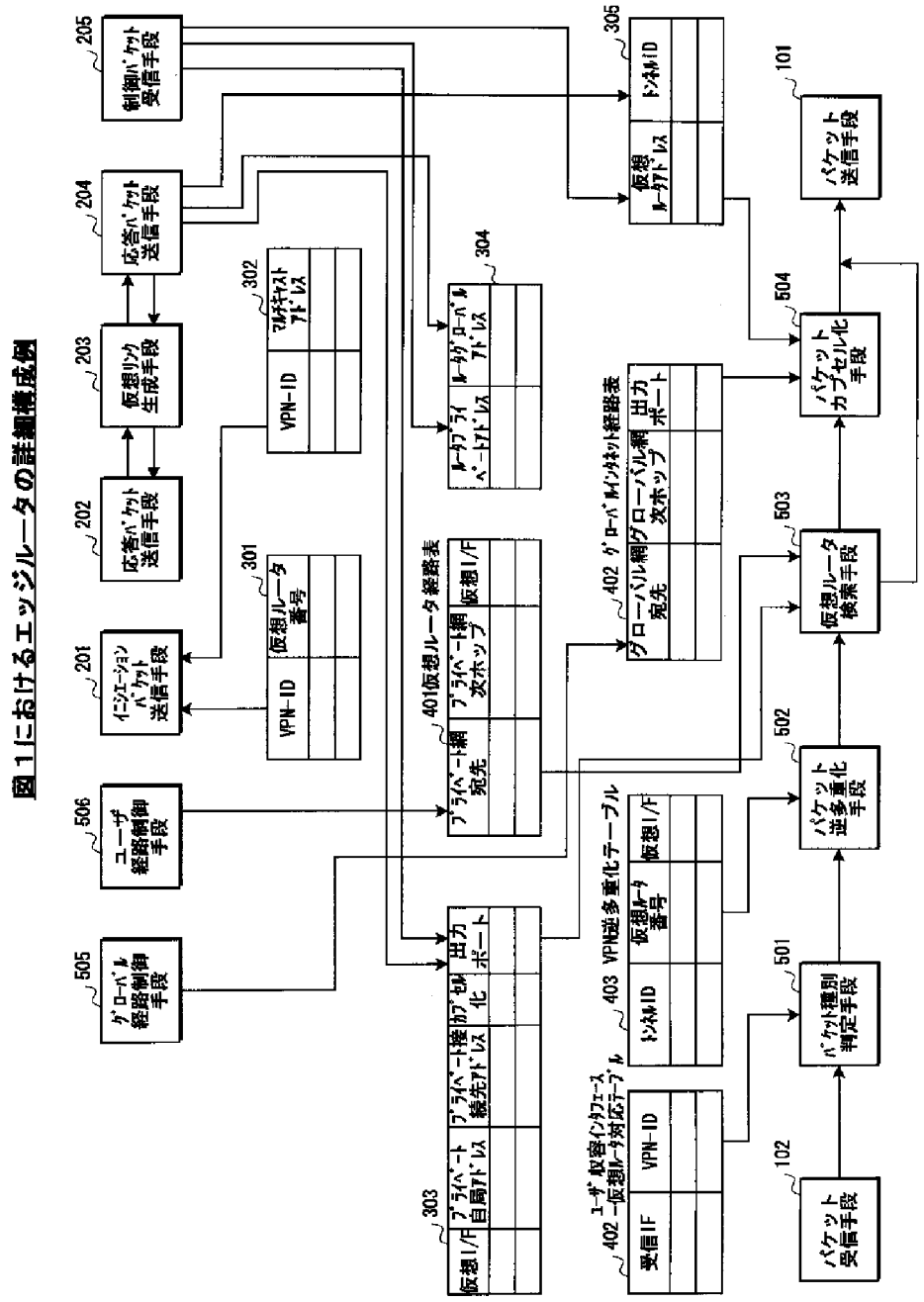
【図２５】

一般的な L2TP トンネル内のパケットフォーマット



【図１３】

図１におけるエッジルータの詳細構成例



【図２０】

エッジルータ PR1 の VPN 逆多重化テーブル

受信トンネル ID	受信セッション ID	受信仮想ルータ	仮想インタフェース
105	200	VPN1-VR1	V1-VR1-VP6
106	201	VPN1-VR1	V1-VR1-VP5
1102	1301	VPN2-VR1	V2-VR1-VP6

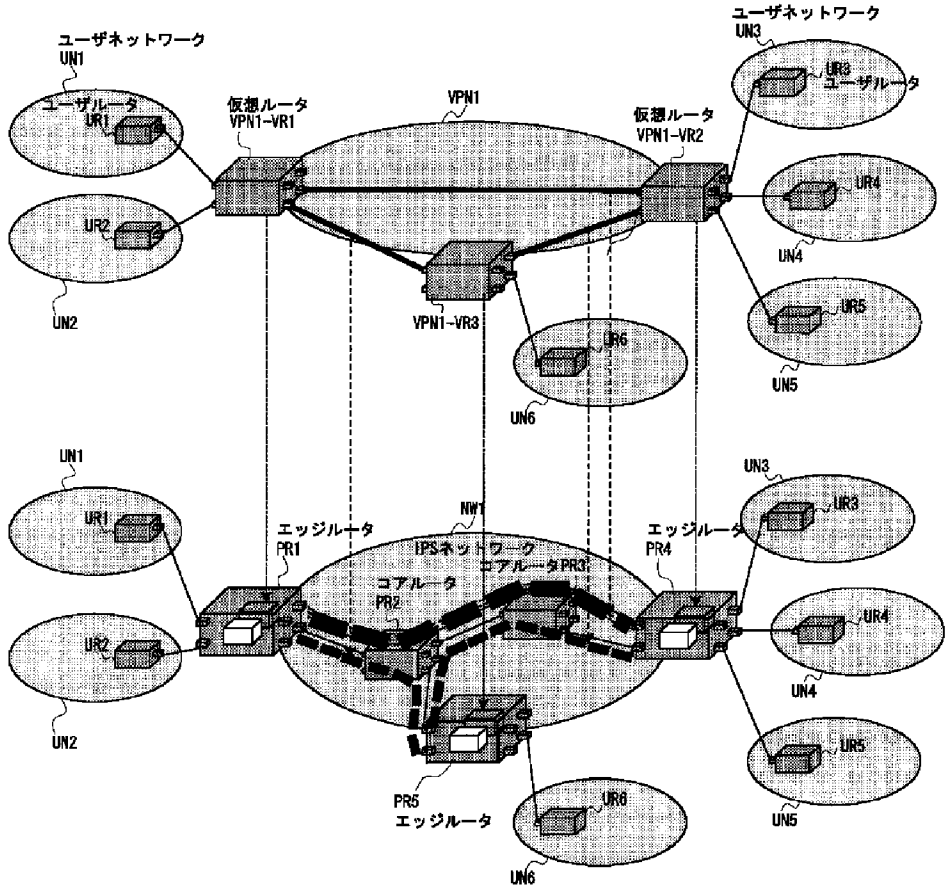
【図２４】

従来の VPN 構成例(1)及び(2)における MPLS トンネル内のパケットフォーマット

Layer 2-header (MAC,PPP ヘッダ等)	転送用 SHIM ヘッダ	VPN 用 SHIM ヘッダ	IP ヘッダ	TCP/UDP ヘッダ等	ユーザデータ

【図２１】

一般的なＶＰＮのグローバルインタネットへのオーバレイ



【図２６】

一般的な IPsec トンネル内のパケットフォーマット(1)

外側 IPv4 ヘッダ	AH ヘッダ	内側 IPv4 ヘッダ	IP 上位層データ(TCP 他)

認証の対象となる範囲

【図２７】

一般的な IPsec トンネル内のパケットフォーマット(2)

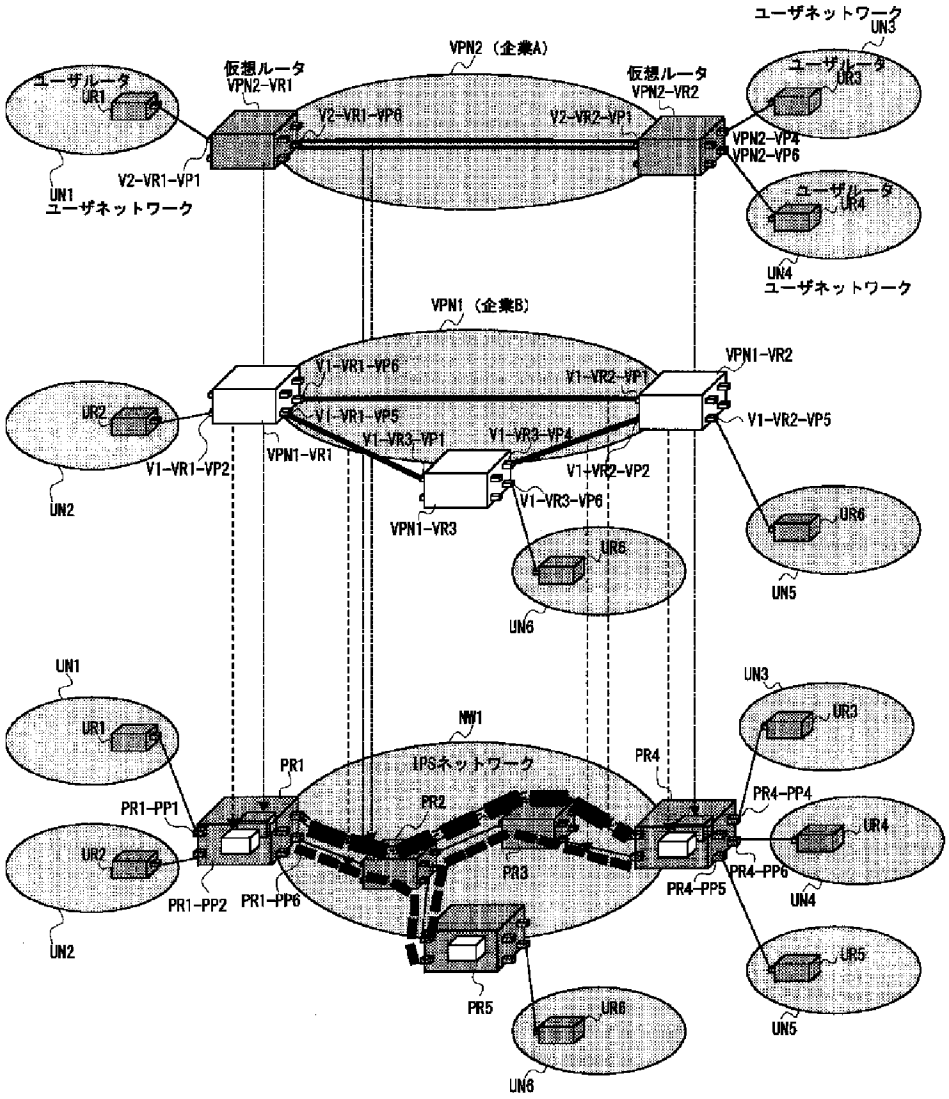
外側 IPv4 ヘッダ	ESP ヘッダ	内側 IPv4 ヘッダ	IP 上位層データ (TCP 他)	ESP トレイラ	ESP 認証ヘッダ

暗号化の対象となる範囲

認証の対象となる範囲

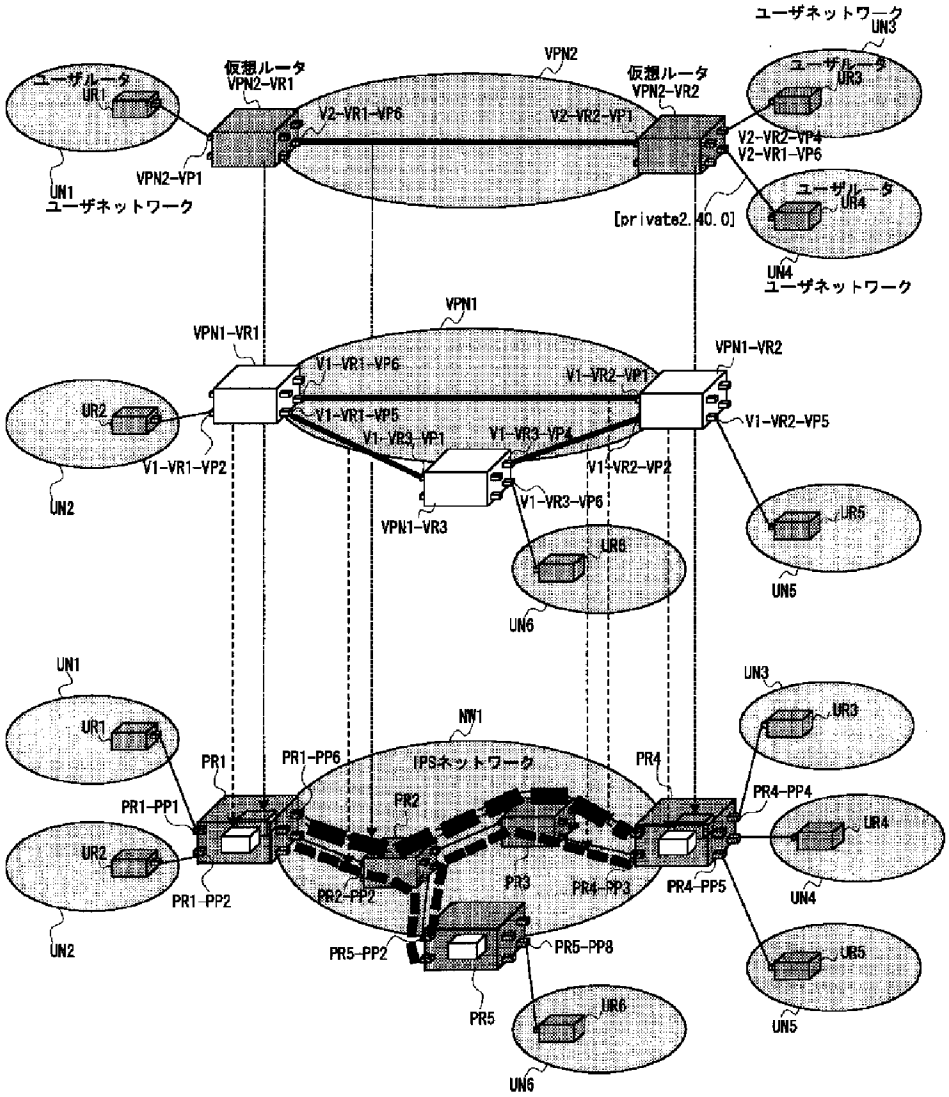
【図２２】

従来のＶＰＮ構成例（１）



【図２３】

従来のＶＰＮ構成例（２）



フロントページの続き

Ｆターム(参考) 5K030 HA08 HC01 HC14 HD03 HD07
LB05 LD06 LD20
5K033 AA03 CB13 CC02 DA05